ACCEPTABLE USE POLICY FOR ELECTRONIC COMMUNICATION NETWORKS

DEFINITIONS

Electronic Communications Networks

This term refers to any system capable of linking computers electronically and includes the following: Local Area Networks (College), Wide Area Networks, Bulletin Boards, Electronic Mail Systems, the Internet and the World Wide Web. CDs, DVDs, memory cards, USB drives and cloud based storage services, when connected to a computer on the College Network are deemed to be a part of the network and will be treated as such. Student laptops are also considered to be part of the network while at the College. The contents of such media, or devices with data storage capabilities, will be subject to the same scrutiny as the rest of the network.

User

Saint Stephen's College provides computer and network facilities to allow students to access and use information sources available on a range of electronic communication networks. Access is conditional on users complying with existing rules and Acceptable Use Policies, which are incorporated in this document.

CONDITIONS AND RULES FOR USE

Acceptable Use

a) Access to Electronic Communications Networks is to facilitate communications in support of research and education, by providing access to unique resources and opportunities for collaborative work. To remain eligible as a user, accessing the College's computer facilities must be in support of and consistent with the educational objectives of Saint Stephen's College.
b) Transmission of any material in violation of any College Policy or Federal/State regulation is prohibited. This includes, but is not limited to, copyright material, and threatening or obscene material.
c) Use for commercial activities is not acceptable. Use for product advertisement or lobbying is also prohibited.
d) Execution of software (which may include, but is not limited to, executable programs, music files and video files) from CDs, USB Drives, any removable media or the Internet is expressly denied on *computer laboratory computers*. Only the software provided on the College network by the College, in the form of icons on the computer desktop, in the Netware Applications Folder or in the 'Start' menu, is permitted to be executed.
e) The College Electronic Communications Networks, including the associated email addresses and email accounts, may not be used to set up or access social media accounts for personal use.
f) Software and files on a student laptop should be appropriate for a school environment.

T: +61 7 5573 8600 | F: +61 7 5573 8688 | E: admin@ssc.qld.edu.au | W: saintstephenscollege.net.au
Reserve Road Coomera Gold Coast Qld 4209 Australia | PO Box 441 Oxenford Qld 4210 Australia
Saint Stephen's College Limited ABN 31 071 134 024 | CRICOS Provider Number 01938G

Privilege

The use of the Internet and the computer network is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of the privilege.

Monitoring

Saint Stephen's College reserves the right to review any computer based material, for example user accounts, fileserver space, email or on media or devices/computers brought into the College, in order to determine whether specific uses of the technology are appropriate. Cloud-based storage may also be reviewed if necessary. In reviewing and monitoring user materials, the College shall respect the privacy of user accounts. However, inappropriate material may be removed without notification. The College also reserves the right to remotely monitor laboratory computer screens to determine the relevance of the work being conducted. Removable media (Optical media, USB drives, memory cards, etc.) found to contain inappropriate material may be confiscated to ensure it is not used within the College. Students taking steps to prevent IT staff from monitoring or controlling a computer provided by the College (e.g. in a computer laboratory) by, but not limited to, switching off the computer to break a connection will be deemed to be inappropriately using the system. *In extreme cases, and after consultation with parents\carers,* individual student laptops may have monitoring software installed. If this happens, the monitoring software will work only when on campus when attached to the College wireless network.

Network Etiquette

All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

a) Be polite. Do not get abusive. (ie. 'put downs'/derogatory language/comments) in your messages to others.

b) Use appropriate language. Do not swear, use vulgarities or any other inappropriate language or graphics. Do not engage in activities which are prohibited under state or federal laws.

c) Keep your personal information, such as your address or phone number, private. This also applies to the private information of students or staff.

d) Note that electronic mail (e-mail) and other systems are not guaranteed to be private. People who operate the system may have access to all mail and communications. Messages relating to or in support of illegal activities will be reported to the authorities and may also result in the loss of other privileges.

e) Use the network in such a way that you do not disrupt its use by others.

f) Communications and information accessible via the network should be assumed to be private property and thus should not be copied or transmitted to others without permission of the owner of the material.

No Warranties

Saint Stephen's College makes no warranties of any kind, whether expressed or implied, for the service it is providing. Saint Stephen's College will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, no-deliveries, incorrect deliveries, or service interruptions caused by the College or by the user's errors or omissions. Use of any information obtained via the Internet/Intranet is at the user's own risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information they obtain, and consider how valid that information may be.

Vandalism and Harassment

a) Vandalism and/or harassment will result in cancellation of user privileges.

b) Vandalism is defined as any malicious attempt to harm, modify or destroy data or hardware of another user of the network. This includes, but is not limited to the uploading or creating of computer viruses or any other type of malicious software.

c) Harassment is defined as the persistent annoyance of another user, or interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted mail and/or 'spam' to multiple recipients.

Encounter of Controversial Material

Users may encounter material which is controversial, and which users, parents, teachers or administrators may consider inappropriate or offensive. While filtering of content on the Internet is performed, on a global network it is impossible to screen or filter all content. It is the user's responsibility not to initiate access to such material or to distribute such material by copying, storing, printing or email. If controversial material is encountered accidentally, the user should navigate away from the material immediately and report the incident to a teacher.

Copyright

Users should not copy and/or redistribute another's work, or use another person's work without correctly acknowledging them and gaining permission if necessary. Users should not break copyright laws. This includes media files of any kind stored on a computer or storage device that connects to the College network

Security

a) Security on any computer system is a high priority, especially when the system involves many users. Users should protect any passwords to ensure system security and their own privilege and ability to continue to use the system. It is recommended that passwords contain a mixture of characters and numbers e.g. *1MyPass23*. Passwords should not be common names, or words that others are likely to guess.

b) If you feel you can identify a security problem on the network, you must notify a System Administrator who may be contacted via the IT Department. Do not demonstrate the problem to other users.

c) Do not use another individual's account.

d) Attempts to log on as a System Administrator will result in cancellation of user privileges. Other penalties may also apply.

e) Attempts to 'hack' into the network or individual workstations will result in cancellation of user privileges. Other penalties may also apply.

f) Attempts to bypass security systems in place on the network will result in disciplinary action. This may include "add-ins" to browsers to bypass Internet filtering, VPN software, anonymizers, etc. and any other software designed for this purpose. Students must use only the browser(s) specified by the College while on campus or while taking part in educational activities associated with the College.

g) Students must use only the wireless network provided by Saint Stephen's College while on campus. Use of Wi-Fi "hotspots', tethering to a mobile phone and/or alternative Wi-Fi networks is not permitted.

h) Any user identified as a security risk, through having a history of problems with this or other computer systems may be denied access to the College network and the Internet by Saint Stephen's College.

Consideration of others

a) Distraction

a. The use of a device should not be a distraction to the teaching and learning of other students and/or staff.

b. Students must have their own headphones and should use them when audio output from their device is necessary.

b) Recording

a. Students are not permitted to record staff or students in any way (audio, video, images, etc.) without first gaining permission of the people involved.

b. This applies to any device, including computers, mobile phones, and cameras.

CONSEQUENCES FOR IMPROPER USE

Any user violating these rules is subject to loss of privileges and possibly other facets of the College's Code of Behaviour/Discipline options.